IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	:	
	:	
vs.	:	1:14CR367-1
	:	
CHRISTOPHER SHANE JENKINS	:	

DEFENDANT'S MOTION TO COMPEL DISCOVERY AND PRODUCTION OF INFORMATION RELATING TO USE OF "IMSI" ELECTRONIC DEVICES

JOHN A. DUSENBURY, JR., Assistant Federal Public Defender and counsel of record for Defendant Christopher Shane Jenkins moves pursuant to Rule 16 of the Federal Rules of Criminal Procedure, the Fourth, Fifth and Sixth Amendments to the Constitution of the United States, and *Brady v. Maryland,* 373 U. S. 83, 87 (1963)for entry of an order directing counsel for the government to disclose whether and to what extent electronic devices capable of identifying the location of a cellular telephone, known as International Mobile Subscriber Identity (IMSI) catchers or cell site simulators were utilized during the investigation in this case.

Based upon information furnished in discovery and information disclosed through independent investigation the undersigned believes that an IMSI catcher or cell site simulator was utilized in this case, and seeks discovery of the following records about such devices, regardless of its name or label:

1. Details concerning the devices, whether in writing or

otherwise concerning:

a. the manufacturer and brand of the device(s) and any equipment used in connection with the device(s);

b. the capabilities of the device(s);

c. descriptions of the information captured by the device(s) and how it was retained.

2. Physical access to any and all such devices used by any federal, state or local law enforcement agency or official.

3. Copies of the raw data produced by the device(s) and utilized by law enforcement.

4. For all the law enforcement agencies and officers involved in this case, copies of any and all

a. arrest reports from any officers who used any device during this case, regardless of whether the device(s) is/are specifically referenced in the report;

b. logs, sign out sheets or other records documenting who used the device(s) and the circumstances surrounding its deployment;

c. training or certification records of the officers that used the device(s);

d. training materials in the possession of law enforcement agencies for the device(s);

e. contracts, memoranda of understanding and agreements, including but not limited to non-disclosure agreements, concerning the device in the possession of, or that bind

the law enforcement agencies involved;

f. administrative or grand jury subpoenas, pen registers, search warrants and any other judicial order, including the application, affidavit and orders applied for, whether granted or not, by law enforcement in this case concerning

I. Christopher Shane Jenkins

ii. Andrew Menjivar

DISCUSSION

The Defendant in this case is charged in a single count bill of indictment with possessing a .40 caliber handgun as a convicted felon in violation of 18 U. S. C.§§ 922(g)(1) and 924(a)(2). The offense is alleged to have occurred on February 4, 2015. Discovery in the case was received by the undersigned on May 13, 2015 and consists of several hundred pages of material. Reports suggest that the firearm in question was recovered from room 108 at the Traveler's Inn at 5906 University Parkway in Winston Salem, NC following a 30 plus hour stalemate between Mr. Jenkins and law enforcement officers from multiple police agencies, including members of "SWAT" (Special Weapons and Tactics) teams from different area law enforcement agencies.

The incident reportedly arose from an encounter on Sunday evening, February 2, 2015 outside a Waffle House in King, NC. Police allege that Mr. Jenkins fled from a King police officer in his car, resulting in a pursuit by the officer. Officers state

that during the pursuit a 911 phone call was made from the Defendant's vehicle stating that a hostage[1] was in the car who would be killed unless officers stopped following. Officers subsequently stopped the pursuit.

Mr. Jenkins turned his cell phone off prior to arriving at the Traveler's Inn in Winston Salem on the morning of the 3rd of February. He neither texted nor called anyone on his or any other phone until approximately 10:00 AM on the morning of the 3rd. At about that time he looked outside his room and saw no police officers in the area. He then placed two telephone calls using his phone, and sent one text message. At approximately 10:30 AM he stepped outside his room and saw between eight and ten police cars establishing a perimeter in front of his room. He stepped back into the room where he remained with his brother until approximately 1:30 PM on Tuesday, February 4th. At that time Andrew Menjivar, the Defendant's brother, left the room and was taken into custody by officers. Mr. Jenkins surrendered to authorities without incident at approximately 3:30 PM on the 4th.

Reports furnished in discovery indicate that at approximately 10:11 AM on the morning of February 3rd the Winston Salem Police Department received a series of anonymous text messages from someone identified only as "BITEBACK" which purported to say that Christopher Jenkins was in room 108 at the Traveler's Inn, "off

[1]Subsequent investigation revealed that the only other occupant of the vehicle was Mr. Jenkins' brother Andrew Menjivar, who at no point during the encounter had been held against his will and was neither harmed nor threatened with injury.

University Parkway." The message continued, "[h]e is wanted in several places for several crimes. Get there quickly he is leaving soon." At approximately 10:28 "BITEBACK" purportedly texted that Mr. Jenkins had a weapon, which he later described as "a 40 handgun", and that he was with his 16 year old brother and driving a silver Nissan. On the basis of this information officers were dispatched to the Traveler's Inn. Responding officers included SWAT officers from the Winston-Salem, Greensboro and High Point Police Departments.

At some point on February 3rd Winston Salem police officers requested the assistance of the North Carolina State Bureau of Investigation in the procurement of an emergency electronic surveillance order authorizing the use of a "hostage negotiator telephone", pursuant to NCGS §15A-290. The device was to be used to communicate with the Defendant from inside his hotel room. The so-called "hostage negotiator telephone" is apparently a telephone equipped with a microphone that enables police to conduct electronic surveillance of sounds coming from inside the room even when the telephone is not in use.

The application for the emergency electronic surveillance order included a sworn affidavit prepared by SBI Special Agent Jay Floyd. The affidavit stated, *inter alia*, that

> ". . . [S]hortly before 11:00 AM on February 3, 2014 Winston Salem Police Officer noticed the suspect vehicle from the all points bulletin in the parking lot of the Travelers Inn located at 5906 University Drive in Winston Salem, North Carolina. . . . The officer who spotted the suspect vehicle

> called for back up. As a second marked unit was arriving . . . a white male, believed to be Christopher Shane Jenkins . . . stepped outside Room 108 and noticed the two marked units. Winston Salem police Department set up a perimeter and began negotiating with Jenkins to release the young man believed to be his hostage."

The affidavit made no reference to a purported anonymous Crimestoppers tip as the means by which the Defendant's location was ascertained. Conversely the undersigned is aware of no police report wherein any officer claims to have seen the Defendant outside his hotel room independent of the so-called Crimestopper's tip.

The undersigned has attempted to obtain information about the identity of BITEBACK the purported anonymous Crimestoppers tipster, and was informed that the government had no information regarding the identity of that individual and furthermore had no way of discovering the person's identity.

Discovery furnished by the government in this case confirms that the process of effecting the Defendant's arrest and that of his brother lasted more than 30 hours, involved officials of the Winston-Salem Police Department, the SBI, the FBI and, as noted, SWAT teams from at least three local police departments. The matter was also reported prominently in the local news media, including on site live reports from television news anchors from near the Traveler's Inn. The government acknowledges having utilized at least one electronic surveillance device capable of surreptitiously monitoring private conversations in hotel rooms.

Given the perceived gravity of the situation, the suspiciously fortuitous coincidence between the receipt of the Crimestopper's "tip" and the Defendant's first use of his cell phone on February 3rd and the absence of any reference whatsoever to the anonymous tip in the application for an order authorizing the electronic surveillance that the government admits to having used, it is at least reasonable to believe that the government used a "stingray" or other electronic device capable of identifying the location of a cellular telephone during the investigation in this case.

Stingrays

"Stingray" is the name for the Harris Corporation's line of "cell site simulator" devices, also called "IMSI catchers". Wireless carriers provide coverage through a network of base stations that connect wireless devices on the network to the regular telephone network. An IMSI catcher masquerades as a wireless carrier's base station, prompting wireless devices to communicate with it. Stingrays are commonly used in two ways: to collect unique numeric identifiers associated with phones in a given location or to ascertain the location of a phone "when the officers know the numbers associated with it but don't know precisely where it is."[2]

Several features of the technology have constitutional implications. The device broadcasts electronic signals that

[2]Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall Street Journal (Sept 21, 2011)

penetrate the walls of private locations not visible to the naked eye, including homes, offices and other private areas of the target and third parties in the vicinity.[3]

The devices can also pinpoint an individual with extraordinary precision, in some cases "within an accuracy of 2 meters."[4] *United States v. Rigmaiden*, 2013 WL 1932800(D. Ariz. May 8, 2013), a tax fraud prosecution is one of the few cases in which the government's use of the device has come to light. In *Rigmaiden* the government conceded that agents used the device while wandering around an apartment complex on foot, and that the device ultimately located the suspect while he was inside his unit. *id.* , at 15.

Stingrays also impact third parties on a significant scale. In particular, they capture information from third parties by mimicking a wireless company's network equipment and thereby triggering an automatic response from all mobile devices on the same network in the vicinity.[5] The government in *Rigmaiden*

---

[3]The devices send signals like those emitted by a carrier's own base stations. *See, e. g.*, Harris Wireless Products Group, Product Description, 1("Active interrogation capability emulates base stations'), http://servv89pn0aj.sn.sourcedns.com/gbpprorg/2600/Harris StingRay.pdf. Those signals "penetrate walls" (necessarily, to provide connectivity indoors). *What You Need to Know About Your Network*, AT&T, http://www.att.com/gen/press-room?pid=14003; *see also* E. H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 The Bell Systems Technical Journal 2719 (1983), http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf.

[4]*See*, e. g. PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12 (device can "locat[e] . . . a target mobile phone within an accuracy of 2 m[eters]".) Http://www.docstoc.com/docs/99662489/GSM-CELLULAR MONITORING-SYSTEMS—PKI-Electronic-#

[5]Hannes Federrath, *Protection in Mobile Communications*, MULTILATERAL SECURITY IN COMMUNICATIONS, 5 (Gunter Muller, *et. al.* Eds., 1999) ("possible to

conceded as much. *id.* at 20.

The devices can also be configured to capture the actual content of phone calls or text messages.[6]

The government has also deliberately failed to disclose crucial details about its use of stingray technology - even in some instances to magistrate judges who oversee and approve electronic surveillance applications. In *Rigmaiden* the government sought court authorization from a Magistrate Judge to use a stingray, but the application did not indicate that the device at issue was a stingray and "did not disclose that the . . . device would capture signals from other cell phones in the area." *Id.*

Stingray technology affronts the constitution in a number of respects. Because of its inevitable impact on third parties it is doubtful that the technology can ever be used in a manner that is consistent with the Fourth Amendment. The Fourth Amendment was "the product of [the Framers'] revulsion against general warrants" that provided British customs officials "blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas*, 379 U. S. 476, 481-82 (1965). Stingrays inevitably gather information about innocent third parties as to whom there is no probable cause.

The government's use of these devices also constitutes a

---

determine the IMSI's of all users of a radio cell.")

[6]Ability, "Active GSM Interceptor:IBIS II - In-Between Interception System - 2nd Generation" ("Real Time interception for Voice and SMS"), http://www.Interceptors.com/intercept-solutions/Active-GSM-Interceptor.html

search within the meaning of the Fourth Amendment. By pinpointing suspects and third parties when they are inside homes and other private locations, stingrays invade reasonable expectations of privacy. *Kyllo v. United States*, 533 U. S. 27, 34 (2001) (thermal imaging to detect heat signature from a home constituted a search); *United States v. Karo*, 468 U. S. 705, 715 (1984) (monitoring of beeper placed into a can of ether that was taken into a residence constituted a search). Because they send a signal that penetrates the walls of private property, stingrays inevitably involve a trespass. *Silverman v. United States,* 365 U. S. 505, 509(1961) (use of "spike mike", a microphone attached to spike inserted into the walls of a house constituted "unauthorized physical penetration into the premises"). Also to the extent that the government uses stingray devices while walking on foot immediately outside people's places of residence to gather information about interior spaces, it impermissibly intrudes on constitutionally protected areas. *Florida v. Jardines*, 133 S. Ct. 1409 (2013). Consequently use of a stingray is presumptively invalid unless the government obtains a warrant predicated on full disclosure of the scope of the electronic surveillance to be undertaken.

Finally the government's obligations under *Brady v. Maryland* and Rule 16 of the Federal Rules of Criminal Procedure extend to information relevant to a Fourth Amendment motion to suppress. The Defendant is therefore entitled to disclosure of the full extent of the electronic surveillance used in this case. "[S]uppression of

material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different." *United States v. Gamez-Orduno,* 235 F. 3d 453, 461 (9th Cir. 2000).

The foregoing constitutes a reasonable basis to believe that electronic devices capable of identifying the location of a cellular telephone, known as Stingrays, International Mobile Subscriber Identity (IMSI) catchers or cell site simulators were used during the investigation in this case. The relevance of such information to the Defendant's ability to effectively prepare a defense in this case has also been established.

WHEREFORE, Counsel for Mr. Jenkins requests that the Court enter an order directing counsel for the government to disclose the information requested herein or alternatively conduct an evidentiary hearing for the purpose of receiving evidence on the issues which arise from this motion.

Respectfully submitted 02 June, 2015.

LOUIS C. ALLEN
Federal Public Defender

/s/ JOHN A. DUSENBURY, JR.
Assistant Federal Public Defender
North Carolina State Bar No. 9201
Attorney for Defendant
301 N. Elm St., Suite 410
Greensboro, NC 27401
Telephone: (336) 333-5455
E-Mail: john_dusenbury@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on this date, I electronically filed the foregoing with the Clerk of the Court, using the CM/ECF system which will send notification of such filing to the following:

Andrew C. Cochrane, Special ASA

Respectfully submitted, this the 2nd day of June, 2015.

LOUIS C. ALLEN
Federal Public Defender

/s/ JOHN A. DUSENBURY, JR.
Assistant Federal Public Defender